TITLE: CRYPTOGRAPHIC ELECTRONIC GIFT CERTIFICATE
CROSS-REFERENCE TO RELATED APPLICATIONS

Not applicable.

BACKGROUND--FIELD OF INVENTION

This invention relates to electronic gift, rebate and incentive certificates that is distributed over public and private computer networks.

BACKGROUND OF THE INVENTION

In recent years there has been a large increase in electronic commerce over open networks such as the Internet; with so many websites offering similar products and services, it is becoming increasingly more difficult for websites to distinguish themselves. One way to increase the conversion of website visitor to customers or to increase business from existing customers it offer them incentives gift and rebate certificates. These certificates offer additional value to shoppers and in many cases is all that is necessary to get the shopper to purchase your goods or services. Today, companies offer gift and rebate certificates that are no more that an email that is sent to a recipient. This email usually contains the monetary value of the certificate and a password. To use the certificate, the recipient must enter the certificate number and or the password at the issuers website. Because the content of the certificate email is not protected, the use of this type of certificate is restricted to the issuing companies website since another website would not have any way of verifying the certificate information the recipient entered.

An example of how it currently works is as follows. If I wanted to offer one thousand dollars in electronic gift certificates to one hundred of my customers with each receiving a ten dollars certificate, I would go to a vendor such as Acme.com and purchase 100 gift certificates for a thousand dollars. Acme would distribute the gift certificates to my customers via email or U.S. post office. My customer is then able to go to Acme's web site and redeem the certificate by entering the appropriate password and or certificate number.

I would never know whether or not a certificate has been redeemed. Acme would benefit from any unredeemed certificates since they were all previously paid for. The vendor (Acme.com) is in full control of the process. Even though I am the certificate issuer, I have to rely on Acme.com to issue the certificates on my behalf.

The electronic gift and rebate certificates of this invention differ from other gift and rebate certificates by allowing the company that pays for the certificates to be the issuing company. It also allows the issuing company to retain savings from any unredeemed certificates. The software of this invention generates, distributes and redeems the certificates. Certificates created by this software invention are data that has been electronically signed using a public private key encryption algorithm (PKI). One such algorithm is described in U.S. Patent 4,405,829 issued to Ronald Rivest, Adi Shamir, and Leonard Adleman. Other public key algorithms such as Diffie-Hellman Algorithm may also be used.

Using PKI (private key) to sign the certificates, this software allows the issuer to distribute its public key to all companies (vendors) that will redeem its certificates. Using the issuer's public key, vendors are able to verify the authenticity of any certificate that is presented as coming from this issuer.

If an issued certificate is never redeemed, the issuer does not have to pay for that certificate which can result in substantial cost saving. The issuer can closely align certificate issuance with its other marketing initiatives for a more effective result. The issuer can use these certificates as a basis for establishing cross marketing campaigns with vendor companies because the certificates are a way of creating customers from the certificate recipient for the vendor company as well.

Upon examination of the software of this invention further advantages will be evident. The software of this requires at least two sets of public private keys to generate certificates. The first set of public keys belongs

to the data reviewer. The Reviewer reviews the information that will be used to generate the certificate such as the name of the receiver, the dollar amount, expiration dates, etc. When the reviewer is satisfied with the accuracy of the information, the reviewer uses his or her private key to sign the data file. The signed review file is handed off to the Issuer. The public key of the Reviewer is installed on the Issuer's computer. The software uses the reviewer's public key that is installed on the issuer's computer to verify the signed review file. When the issuer is satisfied with the accuracy of the signed review file, he or she uses their private key to generate and sign the electronic certificates. Included in each certificate is the issuer's public key. The certificates are then uploaded to a computer server for distribution.

The Issuers public key is distributed to vendors who use it to verify the authenticity of certificates presented to them for redemption. The software encrypts all public keys with a password before distribution to prevent substitution. The encrypted public key is distributed separately from the password to reduce risk.

The Issuer's public key is also installed on the computer server where vendors will send the certificates that have been redeemed for reimbursement. A vendor is reimbursed after the certificate is authenticated with the Issuer's public key.

Before the vendor version of this software redeems a certificate, the software compares the public key of the issuer that is embedded in the certificate with the public key it received from the issuer. If the public keys match, it is used to decrypt the certificate, if not the certificate is rejected. A certificate is accepted only if its decrypted data is formatted correctly. If encrypted data was modified or the public key was substituted the decrypted certificate output will not be formatted correctly and would contain extraneous data.

The vendor software submits the authenticated certificate to the Issuer's computer for reimbursement. Issuer's computer performs a similar check before payment is made to the vendor. Prior arrangements must be made with vendors for credit lines since vendors are supplying goods or services before payment is received.

To facilitate ease of use we have adopted XML as the preferred means of packaging the data elements of a certificate. We have also adopted the W3C (world wide web consortium) electronic signature specification as one means of packaging an electronic gift certificate. This specification is based on the public private key (PKI) encryption technology. We have added additional data elements to the electronic signature to accommodate the needs of an electronic gift, rebate or incentive certificate. More information on W3C electronic signatures can be found at the web address http://www.w3.org/Signature/

SUMMARY

It is an object of this invention to allow companies, individuals and other entities to generate and issue electronic gift and rebate certificates that are redeemable by the issuing and outside companies and to pass all cost saving from unredeemed certificates that would have otherwise gone to a vendor to the issuer.

Additionally, this invention enables electronic gift certificate issuers to issue electronic gift certificates that are redeemable at other companies' websites.

Additionally, this invention allows companies to participate in cross promotion of their business through the use of encrypted electronic gift certificate without the large risk involved with traditional password implemented electronic gift certificates where an unauthorized person could gain access to its password.

Objects and Advantages

Accordingly, beside the objects and advantages of the electronic gift certificate described in the above patent application description, several objects and advantages are

a) to provide an electronic gift, rebate or incentive certificate that does not require the issuer to pay in advance for it, thereby freeing up finances that can be used elsewhere;

b) to allow the issuer to keep the saving from unredeemed certificates since a certificate is paid for only if it is redeemed, yet allow the issuer to receive the benefits from the certificate encouraging the recipient to conduct business with the issuer;

c) to allow the issuer to issue certificates that are redeemable by other organizations and institutions even when the issuer is offline;

d) to allow the issuer to set up collaborative and cross marketing opportunities with other organizations (vendors) using the certificate to introduce the certificate recipient to the vendor. This recipient could become a repeat customer with or without a certificate to the vendor; the issuer could receive payment of fees from the vendor, which would increase the issuer and vendor's financial bottom line.

e) Provide a means to where the issuer and external parties can detect if a certificate is genuine or has been altered using PKI –Public Private key encryption;

f) to reduce the possibility of fraud by requiring at least two people, the reviewer and an Issuer to sign off on the content data that is used to generate electronic certificates before any certificates can be generated;

g) to increase the ease of use by eliminating the need of the certificate recipient to memorize a password or certificate number needed in traditional password certificates;

h) to provide a better means of controlling financial obligations resulting from the issuing of electronic gift certificates by including an expiration date that sets a specific exposure period;

i) to provide increased security by requiring the reviewer and issuer to change their public and private keys frequently thus reducing the chances that the keys used to generate the certificates will be compromised;

j) to provide a means whereby the software used to process the redeemed certificates is provided to the vendors there by reducing the time needed to integrate the processing of the electronic gift certificates and increasing the likelihood that the vendor will participate in the process;

k) The software of this invention when used by the vendor has the ability to set limits on the amount of money the vendor is prepared to advance to the issuer over a specific period of time thereby limiting the financial exposure of the vendor.

Further objects and advantages are the reduced cost of implementing the system described in this invention, which consist primarily of installing software. Taking advantage of most existing computer networks including the Internet will further reduce the implementation cost. Further objects and advantages will become apparent from a consideration of the ensuing descriptions and drawings.

DRAWINGS FIGURES

FIG. 1 shows the process of generating and distributing electronic gift, rebate or incentive certificates.

FIG. 2 shows how and to whom the public keys of the certificate data reviewer and the certificate data Issuer (certificate generator) are distributed.

FIG. 3 shows a customer redeeming an electronic certificate for goods and services and the vendor submitting the electronic certificate for reimbursement.

Reference Numerals In Drawings

10 The certificate data including name of recipient, value of certificate, expiration date etc, which will be used to later generate the certificates

12 The certificate data being reviewed before being electronically signed (encrypted with private key) by the reviewer

14 The reviewer signed certificate data being sent to the certificate data approval person

16 Software uses reviewer's public key to ensure file has not been altered after signing, upon Issuer's satisfaction of the accuracy of the certificate information the certificates are generated and signed using the Issuer's private key

18 Signed certificates are sent to issuer's server software for distribution

19 Certificates are emailed as an attachment to the customer (recipient)

20 Issuers server software distributes certificates as email file attachments or a link to the certificate on the web server software where customer can download certificate

22 Customer receives the certificate as an attachment or downloads the certificate using the link to the certificate in the email

24 Certificates are stored for later comparison before being reimbursed

30 Certificate data reviewer exports public key after generating it on their software

31 Reviewers public key encrypted with a password after exporting

32 Issuer enters password that is used to decrypt reviewers public key before importing it

33 Certificate data Issuer and certificate generator, exports public key after generating it on their software

34 Issuer's public key encrypted with a password is exported

35 Issuers public key is imported onto the vendor's computer to be used to verify certificates that are redeemed

36 Issuers public key is imported onto the issuer's computer to be used to verify certificates that are presented for reimbursement

40 Vendor where customer will redeem electronic certificate

41 The vendor renders Goods or services

42 Customer having electronic certificate on his or her computer

43 Customer uploads electronic certificate file to vendor as payment

44 Vendor presents customers electronic certificate for reimbursement to certificate issuer

45 Certificate issuer verifies certificate its public key and reimburses vendor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to FIG. 1 to FIG. 3, one embodiment of a decryption key management scheme for a ***software*** distribution system according to the present invention will be described in detail.

FIG. 1 shows the process of generating electronic gift, rebate or incentive certificates that are superior to password electronic certificates. A reviewer reviews the data that will be used as the basis of the certificates. Once the reviewer is satisfied with the accuracy of the information the reviewer electronically signs (encrypts the data using his or her private key) before sending it to the Issuer. The software the Issuer is using verifies the signed data using the public key of the reviewer before allowing the Issuer to generate and sign the certificates. If the Issuer is satisfied with the accuracy of the information the Issuer generates and sign the certificates using his or her private key. The certificates are then distributed by email or sent to a computer where the certificates are distributed.

FIG. 2 shows how and to whom public keys are exported. The public key of the reviewer is exported in an encrypted file and sent to the Issuer. The encrypted public key file and the password used to decrypt it are sent by two different channels to reduce the security risk. The Issuer's public key is exported in an encrypted file and is installed on the vendor's and the issuers' computers.

Fig 3 shows a customer redeeming an electronic incentive certificate for goods and services. The certificate is residing on the customer's computer in a electronically signed file. When the certificate is presented to the vendor, the vendor uses the public key of the Issuer to verify the integrity of the certificate. If the certificate has not been altered the certificate is presented to the issuer for reimbursement. If the issuer using the Issuer's public key verifies the certificate the vendor is reimbursed the value of the certificate.

Advantages

From the description above, a number of advantages of the electronic incentive certificates become evident;

(a) When implementing electronic incentive certificates it is more cost effective for the certificate issuer to manage the certificate issuance and distribution process instead of relying on vendors since unredeemed certificates do not cost the issuer any money whereas if the vendor issued the certificates the vendor would be the one reaping the benefits of any unredeemed certificates.

(b) Electronic certificates that are created using public private keys are more secure since the private key that is used to generate the certificate is never distributed.

(c) Issuers can issue certificates that are redeemable at other vendors website or companies.

(d) The posibility for fraud is reduced because a minimum of two individuals are required to review the file that is used to generate the certificate.

(e) The certificate recipient does not have to remember passwords or serial numbers which makes these electronic incentive certificates easier to use than those requiring passwords.

(f) Vendors can redeem a certificate without having to send it to the issuer for authentication.

(g) Issuers can set up cross marketing oppurtunities with with vendors.

(h) The software of this invention when used by the vendor has the ability to set limits on the amount of money the vendor is prepared to advance to the issuer over a specific period of time thereby limiting the financial exposure of the vendor.

Operation

Generating electronic incentive certificates require two sets of public private encryption key pairs to be created. One key pair belongs to the reviewer and the other to the certificate issuer. To electronically sign an electronic incentive certificate, the private key of issuer is used to encrypt certificate data. To verify a certificate the corresponding issuers public key is used to decrypt the certificate which is then checked for content and format. If the decrypted file is formatted correctly the verification passes.

First, someone working for the certificate Issuer prepares a file containg the names, email adresses, monetary value, expiration date, etc of each certificate. The file is then sent to a reviewer who reviews it for accureacy. If the file is accurate the reviewer uses his or private encryption key to electronically sign the file. The reviewer then sends the signed file to an Issuer who will also review the file for accuracy before generating and signing each electronic certificate using his or her private key.

Before the Issuer is allowed to generate and sign each certificate, the Issuer's software uses the reviewer's matching public key that was imported on the Issuers computer to verify that the signed file has not been altered. After generating the certificates they are distributed electronically to the recipients.

The public key of the certificte Issuer is distributed to vendors and is also installed on the issuers computer where vendors will present redeemed certificates for reimbursement. Before a certificate is reimbursed it is verified using the Issuer's public key. The vendors also use the Issuer's public key to verify that the certificate has not been altered before redeeming it.

Conclusion, Ramifications and Scope

Accordingly, the reader will see that our encrypted electronic incentive certificate is more secure and economical to use that traditional password based electronic incentive certificates. It has additional advantages in that

- It does not require the installation of additional hardware so it can be used on most computers with no modifications necessary;
- Encrypting each certificate significantly reduces the chance of it being altered without detection;
- It has a built in expiration date allowing the issuer to control the lifespan of a certificate and thus control the issuer's financial exposure (obligation);
- A multitued of public private encryption algorithm can be used to implement the cryptographic functions such as RSA from RSA Security Inc, Triple DES;
- Vendors can verify an electronic certificate that is being redeemed without contacting the issuer, allowing certificates to be redeemed even when no communication is possible with the issuer;
- Certificate issuer retains savings and marketing benefits when an issued certificate is not redeemed;
- A password can be added for additional security but can be eliminated so the certificate recipients do not have to memorize password or serial numbers making our electronic gift certificates easier to use than cetificate implemented using passwords;
- The software of this invention when used by the vendor has the ability to set limits on the amount of money the vendor is prepared to advance to the issuer over a specific period of time thereby limiting the financial exposure of the vendor.